

Henna Jansson

**ACTIVE DIRECTORYN KÄYTTÖÖNOTTO - CASE MONDO MINERALS B.V.  
BRANCH FINLAND**

Opinnäytetyö  
Kajaanin ammattikorkeakoulu  
Luonnontieteiden ala  
Tietojenkäsittelyn koulutusohjelma  
Kevät 2009



**Kajaanin**  
**ammattikorkeakoulu**

## OPINNÄYTETYÖ TIIVISTELMÄ

Koulutusala Luonnontieteiden ala	Koulutusohjelma Tietojenkäsittely
Tekijä(t) Henna Jansson	
Työn nimi Active Directoryn käyttöönotto - Case Mondo Minerals B.V. Branch Finland	
Vaihtoehtoiset ammattiopinnot Järjestelmän ylläpito	Ohjaaja(t) Timo Partanen
	Toimeksiantaja Mondo Minerals B.V. Branch Finland
Aika Kevät 2009	Sivumäärä ja liitteet 36
<p>Tämän opinnäytetyön tarkoituksena oli suunnitella ja toteuttaa Active Directory -verkkopalvelu. Työn toimeksiantajana on Mondo Minerals B.V. Branch Finland. Yritys on Sotkamossa Korholanmäellä, sekä kahdella muulla paikkakunnalla Suomessa toimiva, talkkituotteita valmistava yritys. Yrityksen palveluksessa työskentelee noin 170 henkeä. Suurin osa yrityksen työasemista ja palvelimista, noin 120 sijaitsee Sotkamon tehtaalla.</p> <p>Opinnäytteen tavoitteena oli luoda Mondo Mineralsin käyttötarkoituksiin sopiva Active Directory -verkkopalvelu. Ennen Active Directory -verkkoa yrityksen käytössä oli Novell Netware -verkkopalvelu, josta haluttiin siirtyä pois. Active Directory -verkkoon päädyttiin osaksi sveitsiläisen omistajan myötä, joka halusi ottaa Active Directoryn käyttöön Netware -verkon sijaan.</p> <p>Teoriaosuudessa on käsitelty aktiivihakemiston perusominaisuuksia. Lisäksi on selvitetty mitä tulisi huomioida Active Directory -verkon toteutuksessa. Verkkopalvelua, sen tarjoamia mahdollisuuksia ja hyötyjä on pyritty käsittelemään järjestelmän ylläpitäjän näkökulmasta.</p> <p>Käytännönsuudessa on kerrottu, kuinka Active Directory -projekti toteutettiin Mondo Mineralsilla. Osuudessa on kerrottu verkkopalvelun asentamisesta, suunnittelusta sekä toteutuksesta. Käyttöönotto toteutettiin kaikilla kolmella paikkakunnalla Suomessa: Sotkamo, Vuonos ja Helsinki. Pohdinnassa on syvennytty analysoimaan projektin eri vaiheita, sekä aktiivihakemiston tulevaisuutta yrityksen käytössä.</p> <p>Verkon rakenteiden suunnittelu alkoi vuoden 2006 kesällä. Lopullinen suunnittelu ja toteutus tapahtui vuoden 2008 kesään mennessä. Active Directoryn täydellinen käyttöönotto toteutui kesän 2008 aikana, jolloin Novell Netware oli poistettu käytöstä ja yrityksen kaikki tietokoneet käyttivät aktiivihakemiston palveluja.</p>	
Kieli	Suomi
Asiasanat	Active Directory, aktiivihakemisto, verkkopalvelu
Säilytyspaikka	<input checked="" type="checkbox"/> Kajaanin ammattikorkeakoulun Kaktus-tietokanta <input checked="" type="checkbox"/> Kajaanin ammattikorkeakoulun kirjasto

School Business	Degree Programme Business Information Technology
Author(s) Henna Jansson	
Title Inauguration of Active Directory, Case: Mondo Minerals B.V. Branch Finland	
Optional Professional Studies Systems Maintenance	Instructor(s) Timo Partanen
	Commissioned by Mondo Minerals B.V. Branch Finland
Date Spring 2009	Total Number of Pages and Appendices 36
<p>The purpose of this thesis is to design and execute the Active Directory network service. The thesis was commissioned by Mondo Minerals B.V. branch Finland located in Sotkamo Korholanmäki and also in two other locations in Finland. Mondo Minerals B.V. is a producer of talc products. The company has about 170 employees. The majority of the approximately 120 servers and workstations of the company are in Sotkamo.</p> <p>The aim of this thesis was to create the Active Directory network service for Mondo Minerals. They were using the Novell Netware service earlier, but wanted to convert to using the Active Directory. One of the reasons to this was the new owner of the company.</p> <p>The goal of the theoretical part was to study the basic features of the Active Directory. In this part, it was studied what kind of factors should be considered in the implementation of the Active Directory service. The potential and the benefits of the Active Directory were examined from the administrator's point of view.</p> <p>The practical part tells how the Active Directory project was implemented in Mondo Minerals B.V. Finland. The installation, design and implementation of the Active Directory are discussed in this part. The implementation was carried out in three localities in Finland: Sotkamo, Vuonos and Helsinki. The conclusion of the thesis analyzes all the parts of the project and the future of the Active Directory in Mondo Minerals.</p> <p>The design of the Active Directory started in summer 2006. The design and implementation was completed by the summer of 2008. The inauguration of the Active Directory took place in summer 2008 and by that time Novell Netware was out of use and all the computers and servers of Mondo Minerals were using the services of the Active Directory.</p>	
Language of Thesis      Finnish	
Keywords	Active Directory, network service
Deposited at	<input checked="" type="checkbox"/> Kaktus Database at Kajaani University of Applied Sciences <input checked="" type="checkbox"/> Library of Kajaani University of Applied Sciences

## ALKUSANAT

Haluan lämpimästi kiittää perheeni jäseniä, jotka ovat aika ajoin vauhdittaneet opintojeni ja opinnäytteeni loppuun suorittamista.

Kiitos Mondo Minerals B.V. Branch Finlandille opinnäytetyöaiheesta, sekä työharjoittelupaikasta syksyllä 2006.

Kiitokset myös opinnäytetyöni ohjaajalle, Timo Partaselle, ohjauksesta.

Sotkamossa 18. Toukokuuta 2009.

Henna Jansson

## SYMBOLILUETTELO

### ACTIVE DIRECTORY

Aktiivihakemisto

Active Directory on Microsoftin toteutus verkkopalvelusta.

DNS Domain Name System

### DOMAIN

Toimialue

### EXTRANET

Verkkopalvelu

Extranet on palomuurin ulkopuolella toimiva, yrityksen tai yhteisön käyttöön tarkoitettu.

### FOREST

Metsä

Forest on toimialueiden muodostama kokonaisuus.

GPO Group Policy Objekt, ryhmäkäytäntö -objekti

### INTRANET

Verkkopalvelu

Intranet on palomuurin sisäpuolella toimiva organisaation sisäiseen käyttöön tarkoitettu, internetteknologiaan perustuva verkkopalvelu tai -sivusto.

IP Internet Protocoll, Internet protokolla

## KERBEROS

Tunnistusmenetelmä

Menetelmän jonka avulla käyttäjät voivat todistaa henkilöllisyytensä verkossa.

LAN Local Area Network, nopea lähiverkko

OU Organisational unit, organisaatioyksikkö

Ominaisuus jolla voidaan ryhmitellä Active Directory -toimialueen objekteja paremmin hallittaviin kokonaisuuksiin.

## SCHEMA

Kaava

Malli jolla kuvataan toimialueella esiintyvien objektien suhteita.

## SECURE CHANNEL

Vartioitu kanava

Varmistaa tiedon siirron luotettavasti.

SITE Toimipaikka

Toimipaikka on IP -aliverkkojen muodostama kokonaisuus.

## TCP/IP

Transmission Control Protocol/Internet Protoco

TCP/IP on internet -liikennöinnissä käytettävä standardi verkkoprotokolla.

UAS User Account System

UPN User Principal Name, ensisijainen kirjautumistunnus

WAN Wild Area Network, nopea laajaverkko

## SISÄLLYS

1 JOHDANTO	1
2 ACTIVE DIRECTORY	2
2.1 Active Directory toimialueen suunnittelu	2
2.2 Organisaatioyksiköt	6
2.3 Toimipaikat	9
2.4 Active Directoryn asentaminen ja käyttöönotto	9
2.5 Toimialueen hallinta	11
3 JÄRJESTELMÄN YLLÄPITO	20
3.1 Active Directory järjestelmäylläpidossa	20
4 MONDO MINERALS B.V.	22
4.1 ATK -organisaatio	22
5 ACTIVE DIRECTORYN TOTEUTUS MONDO MINERALSILLE	24
5.1 Active Directoryn käyttöönotto	27
5.2 Dokumentointi	30
5.3 Case -projektin yhteenveto	31
6 YHTEENVETO	33
LÄHTEET	35

## 1 JOHDANTO

Tämä opinnäytetyö on tehty Mondo Minerals B.V. Branch Finlandille kevään 2009 aikana. Työn toiminnallinen osuus on kuitenkin suoritettu jo keväällä 2008 ja Active Directory -verkkopalvelu on otettu käyttöön kevään ja kesän 2008 aikana. Projektin tarkoitus oli saada Mondon käyttötarkoitukseen sopiva Active Directory -verkko käyttöön mahdollisimman pian.

Mondo Minerals B.V. on monikansallinen talkkituotteita valmistava yritys. Sen toiminta on keskittynyt Keski- ja Länsi- Eurooppaan, jossa sillä on vahva asema paperialalla. Mondo Minerals B.V. Branch Finland on Suomessa kolmella paikkakunnalla toimiva yritys. Yrityksellä on kaksi tuotantolaitosta Suomessa sekä konttori Helsingissä. Tehtaat sijaitsevat Outokummussa ja Sotkamossa, jossa toimiva tehdas on maailman suurin talkkitehdas.

Yrityksen palveluksessa työskentelee yhteensä noin 170 henkilöä. Yrityksen palveluksessa on kaksi järjestelmän ylläpitäjää, he työskentelevät Sotkamossa. Sotkamossa sijaitsee myös suurin osa yrityksen käytössä olevista työasemista sekä palvelimista, noin 120 yhteensä.

Työn teoriaosuudessa on käsitelty aktiivihakemiston perusominaisuuksia, sekä mitä tulisi ottaa huomioon toteutettaessa Active Directory -verkkoa. Active Directory tarjoaa monia järjestelmän ylläpitäjää helpottavia työkaluja. Hyvin suunniteltuna aktiivihakemisto tekee verkon hallinnasta todella helppoa. Merkittävin hyöty ylläpitäjälle on ylläpidon keskittäminen yhteen paikkaan. Käytännössä tämä tarkoittaa sitä, että jokaista tietokone- tai käyttäjätiliä ei tarvitse hallinnoida yksitellen, vaan asetusten hallinnointi onnistuu organisaatioryksiköittäin.

Työn toinen luku käsittelee Active Directory -teoriaa. Kolmannessa luvussa kerrotaan lukijalle, mitä järjestelmän ylläpito käytännössä tarkoittaa. Ylläpidon jälkeen siirrytään esittelemään case -yritystä, Mondo Minerals B.V.:tä. Luvussa esitellään koko yritystä sekä Suomen toimipaikkoja (Branch Finland), joille Active Directory -verkko toteutettiin. Viidennessä luvussa kerrotaan lisää käytännöntyön toteutuksesta. Lopuksi yhteenvedossa on pohdittu verkon käyttöönoton onnistumista sekä sen tulevaisuudessa tarjoamia mahdollisuuksia.



## 2 ACTIVE DIRECTORY

Active Directory eli aktiivihakemisto on Microsoftin toteutus hakemistopalvelusta, jonka avulla voidaan tehokkaasti hallita verkon resursseja. Active Directory on Microsoft Server 2003:n ydin. Se on tietokanta, joka sisältää tietoa käyttäjistä, tietokoneista ja verkkoresursseista. (Kivimäki 2005, 1; Stanek 2003, 133.)

”Active Directory -teknologia perustuu standardeihin Internetin protokolliin, sen avulla voidaan määrittää verkon rakenne selkeästi” (Stanek 2003, 133). Järjestelmänylläpitäjän kannalta AD:ssä on kysymys hajautetun järjestelmän keskitetystä hallinnoinnista. Käytännössä tämä tarkoittaa sitä, että loogisesti yhdessä paikassa sijaitsevia objekteja voidaan hallita erilaisilla hallintatyökaluilla yhdestä paikasta käsin. Näitä hallintatyökaluja ovat erilaiset hallintakonsolit, kuten esimerkiksi Active Directory Users and Computers -konsoli. Active Directory vähentää ylläpidettävien hakemistojen määrää, koska objekteja voidaan hallita yhtenäisillä rajapinnoilla ja työkaluilla. (Kivimäki 2005, 6.)

Perinteisen määrittelyn mukaan hakemistopalvelu (directory service) eroaa hakemistosta (directory) siten, että se sisältää sekä hakemiston tietovaraston (tietokannan), kuin myös palvelut, joilla päästään käsiksi tietovarastoihin. (Kivimäki 2005, 1.)

Active Directory ei varsinaisesti näy loppukäyttäjälle. Käyttäjä voi kuitenkin hyödyntää verkkopalvelun tarjoamia resurssienetsintä tai muita käyttöä helpottavia toimintoja. Tällaisia toimintoja ovat esimerkiksi kirjoittimien etsiminen ja verkkohakemistojen käyttö. (Kivimäki 2005, 1.)

### 2.1 Active Directory toimialueen suunnittelu

Active Directory toteutukseen liittyy useita suunnitteluprosessissa huomioon otettavia tekijöitä. Toteutusta suunniteltaessa on otettava huomioon DNS -nimiavaruus (domain name system). Nimiavaruus sisältää toimialuehierarkian, luottosuhteet, globaalin luettelon ja replikoinnin. Lisäksi suunnitellaan organisaatioyksiköt (organisational units), jotka myös nekin kuuluvat nimiavaruuteen. Laajempaa verkkoa suunniteltaessa on syytä ottaa huomioon myös

toimipaikat (sites), niiden avulla optimoidaan sisäänkirjautumis- ja replikointiliikennettä. (Kivimäki 2005, 8; Turunen 2006, 22.)

Active Directory käyttää DNS:iä (domain name system) paikannuspalveluna. DNS on standardi Internetin palvelu, johon Active Directoryn nimiavaruus perustuu. Nimiavaruus on rajallinen alue, jonka avulla nimi muutetaan numeeriseksi TCP/IP -osoitteeksi (Transmission Control Protocol/Internet Protocol). DNS järjestee tietokonejoukot hierarkisiksi toimialueiksi, sekä mahdollistaa useiden toimialueiden liittämisen puurakenteeksi. (Kivimäki 2005, 8; Stanek 2003, 133; Turunen 2006, 22.)

Active Directoryn nimiavaruus määrittää organisaation ylimmän tason toimialueenimen (forest root domain). Jyrki Kivimäen mukaan ehkä tärkein päätös nimiavaruuteen liittyen on päättää, että käyttääkö Active Directory samaa nimiavaruutta, kuin mikä DNS -nimiavaruus (Internet-toimialueenimi) on jo mahdollisesti rekisteröity organisaation käyttöön. Toinen nimiavaruuteen liittyvä seikka on, että luodaanko tai säilytetäänkö erillinen sisäinen nimiavaruus eli intranet (palomuurin sisäpuolella) ja ulkoinen julkinen nimiavaruus eli extranet (palomuurin ulkopuolella) vai halutaanko ne yhdistää. Toimialueen nimeäminen vaikuttaa kaikkiin Active Directoryn objekteihin. (Kivimäki 2005, 8.)

Jos organisaation sisäinen ja ulkoinen nimiavaruus ovat erilliset, niin halutessaan organisaatio voi varata molemmat nimet Internetin DNS-rekisteröijältä. Mikäli molemmat nimet rekisteröidään, niin tällöin toinen julkinen verkko ei voi varata organisaation sisäistä nimeä. (Kivimäki 2005, 8.)

Yksi mahdollisuus on käyttää esimerkiksi ylimmän tason toimialue tunnusta .local eli rekisteröimätöntä sisäisen verkon nimeä. Näin voidaan luoda erillinen sisäinen nimiavaruus esimerkiksi yritys.local. Tällöin Internetissä käytetään nimeä yritys.fi ja intranetissä nimeä yritys.local. (Kivimäki 2005, 8.)

Kun sisäisellä ja ulkoisella nimiavaruudella on käytössä eri nimet, on resurssit helppo erottaa toisistaan. Huomattava etu on myös se, että välttämättä ei tarvitse tehdä jo käytössä olevaan julkisen verkon DNS -palvelimeen mitään lisämäärittäyksiä. Myös verkon hallintatyö helpottuu, kun päällekkäistä ja kaksinkertaista ylläpitoa ei tarvita. Samalla myös välityspalvelinta (proxy) käyttävien asiakkaiden konfigurointi yksinkertaistuu, kun rajoitusluettelossa (exclusion list) tarvitaan vain yksi nimi tunnistettaessa ulkoisia resursseja. (Kivimäki 2005, 8.)

”Kaikki Active Directory -toimialueet ovat liittyneet johonkin metsään (forest)” (Kivimäki 2005, 9). Jo yksikin toimialue muodostaa metsän, johon kuuluu vain yksi toimialue. Metsään voi kuulua myös useampia toimialueita. Toimialueella voi olla vain yksi ohjauspalvelin. (Kivimäki 2005, 9.)

Toimialue luodaan Windows Serverille Active Directory -asennuksen yhteydessä. Asennuksen aikana nimetään luotava toimialue, josta tulee metsän juuritoimialue (forest root domain). Samassa yhteydessä toimialueesta tulee nimiavaruuden ensimmäinen toimialue. Ensimmäisellä toimialueella on enemmän valtuuksia ja suurempi merkitys, kuin muilla metsän toimialueilla. Juuritoimialueen nimeäminen on syytä suunnitella huolellisesti, sillä sen uudelleen nimeäminen tai poistaminen on erittäin haasteellista tai miltei mahdotonta. (Kivimäki 2005, 9; Partanen 2007.)

Samaan metsään kuuluvilla toimialueilla on yhteistä esimerkiksi seuraavat seikat:

- Kaikissa metsän toimialueissa on käytettävissä Kerberos-tunnistusmenetelmä. Eli käyttäjä voi kirjautua minkä tahansa toimialueen käyttäjätillillä (user account), mihin tahansa metsän toimialueeseen. Samalla käyttäjälle voidaan antaa oikeudet toisen toimialueen resursseihin. Käyttäjän kirjautumistunnus (User Principal Name) on käytössä koko metsässä.
- Kaava (schema), eli rakenne on yhtäläinen kaikissa metsän toimialueissa. Schema Master -roolin omaava palvelin hallitsee rakennetta. Oletuksena tämän roolin saa toimialueen ensimmäinen asennettu ohjauspalvelin.
- Yleinen luettelo (global catalog) on käytössä metsän laajuisesti. Myös yleistä luetteloa ylläpitää oletuksena ensimmäinen asennettu ohjauspalvelin. Luetteloa voi kuitenkin ylläpitää myös useampi, kuin yksi ohjauspalvelin.
- Enterprise Admins -ryhmän jäsenillä on oikeus muokata kaikkien toimialueiden ohjauspalvelimia. Enterprise Admins -ryhmä on oletuksena mukana kaikkien toimipaikkojen paikallisessa Administrator -ryhmässä.
- Tunnistetut käyttäjät -ryhmä (authenticated users) on voimassa metsän laajuisesti.

- Metsien (forest) liittäminen toisiinsa onnistuu luottosuhteiden avulla. (Kivimäki 2005, 51-52.)

Toimialueilla on omat toimintatasonsa kuin myös jokaisella metsällä (forest functional level). Windows Server 2003:en Active Directory tarjoaa monia eri toimintatasoja (functionality level) vanhempien palvelinkäyttöjärjestelmien Windows NT- ja Windows 2000- ohjauspalvelinten tukea varten. Toimintatasot ovat olleet käytössä jo Windows 2000 Server -käyttöjärjestelmässä, mutta tuolloin niistä käytettiin nimitystä toimintatila (domain mode). (Kivimäki 2005, 52-53.)

#### Active Directoryn toimintatasot

Windows 2000 Mixed Mode (Windows 2000 -sekatila). Tämä tila on kaikilla uusilla toimialueilla. Sekatila tukee sekä Windows 2000 Server -, että Windows Server 2003 -käyttöjärjestelmien ohjauspalvelimia ja lisäksi Windows NT -varaohjauspalvelimia. Sekatilassa toimivat toimialueet eivät voi käyttää useita uusimpia Active Directoryn ominaisuuksia, kuten esimerkiksi: universaaleja ryhmiä, ryhmätyypin muunnosta, ohjauspalvelinten uudelleen nimeämistä, sisäkkäisiä paikallisia ryhmiä, kirjautumisleimojen (logon stamp) päivityksen replikointia tai Kerberosin KDC -avainversionumeroita. (Kivimäki 2005, 53-56.)

Windows 2000 Native Mode (Windows 2000 -natiivitila). Natiivitilassa ei tueta Windows NT -ohjauspalvelimia, vaan vain Windows Server 2003 - ja Windows 2000 Server -ohjauspalvelimia. Tässä tilassa toimivissa toimialueissa ei voida käyttää kirjautumisleimojen päivitystä, toimialueen ohjauspalvelimien uudelleen nimeämistä, eikä Kerberosin KDC -avainversionumeroita. (Kivimäki 2005, 53 – 56.)

Windows Server 2003 Interim Mode (Windows Server 2003 -välitila). Tila muistuttaa Windows 2000 -sekatilaa, mutta välitilassa Active Directory tukee vain Windows Server 2003 -ohjauspalvelimia ja Windows NT -varaohjauspalvelimia. Välitila mahdollistaa NT -toimialueiden päivittämisen suoraan Windows Server 2003 -toimialueeseen ilman 2000 Server -vaihetta. (Kivimäki 2005, 53 – 56.)

Windows Server 2003 Mode (Windows Server 2003 -tila). Taso tukee Windows Server 2003 -ohjauspalvelimia. Toimialueella on mahdollista käyttää kaikkia Active Directory 2003:n mukana tulleita uusia ominaisuuksia. Näitä ominaisuuksia ovat mm. sisäkkäiset ja universaalit

ryhmät, toimialueen ohjauspalvelinten uudelleen nimeäminen, kirjautumisleimojen päivittäminen, ryhmätyyppien muunnos ja Kerberosin KDC -avainversionumerot. Lisäksi Active Directory voi hyödyntää yleisten hakemistojen tai yksittäisten ryhmien jäsenten kehittyneimpiä replikointimahdollisuuksia. Mikäli kaikki metsän toimialueet on nostettu 2003 -tasolle, ei niitä enää voi palauttaa muille toimitasoille takaisin. (Kivimäki 2005, 53 – 56.)

## 2.2 Organisaatioyksiköt

”Organisaatioyksikkö on Active Directory -toimialueiden ominaisuus, jonka avulla toimialueen objekteja voidaan ryhmitellä helpommin hallittaviin kokonaisuuksiin.” (Kivimäki 2005, 368.) Organisaatioyksikkö on säilö, joka voi sisältää mitä tahansa toimialueen objekteja. Objekteja ovat esimerkiksi: käyttäjätilit, käyttäjäryhmät ja kirjoittimet. Organisaatioyksiköitä voidaan tehdä, kun halutaan jakaa käyttäjäryhmiä, resursseja tai käyttäjiä koskevia järjestelmällisiä oikeuksia. Organisaatioyksiköt mahdollistavat sen, että paikallisille tukihenkilöille tai käyttäjille ei tarvitse antaa koko toimialueen laajuisia hallinto-oikeuksia, vaan oikeudet voidaan antaa harkitummin vain johonkin tiettyyn organisaatioyksikköön. (Kivimäki 2005, 10 ja 337.)

Organisaatioyksiköiden käyttö ei ole pakollista, mutta ne on suunniteltu helpottamaan järjestelmänhallintaa. Tarvittaessa organisaatioyksikkörakennetta voidaan muuttaa ja objekteja voidaan siirtää yksiköiden välillä. Mikäli organisaatioyksiköitä ei kuitenkaan haluta käyttää voidaan käyttäjätilit lisätä Users -kansioon alle ja tietokonetilit Computers -kansioon, näihin kansioihin ei kuitenkaan voida kohdistaa ryhmäkäytäntöjä. Oletuksena Active Directory -toimialueella on yksi organisaatioyksikkö (Domain Controllers) siihen on linkitetty Default Domain Controllers Policy -ryhmäkäytäntöobjekti. Organisaatioyksikkörakenteen tulisi kuitenkin perustua käytännön hallinnallisiin tarpeisiin. (Kivimäki 2003, 337; Kivimäki 2005, 10 ja 368.)

Ennen objektien luomista Active Directoryyn tulisi suunnitella sekä luoda organisaatioyksiköt, joihin objektit sijoitetaan. Organisaatioyksiköiden luomisessa tulisi huomioida seuraavia seikkoja:

- Organisaatioyksikkö ei näy käyttäjälle. Käyttäjä kirjautuu toimialueelle, ei organisaatioyksikköön.

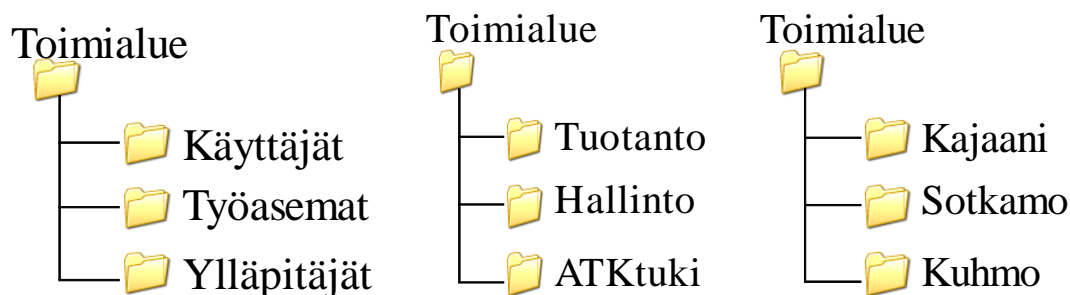
- Organisaatioyksiköiden tulisi heijastaa organisaation tai yrityksen liiketoiminnallista rakennetta. Näin saadaan aikaan järkevästi hallittavia kokonaisuuksia toimialueelle.
- Käyttäjätilien ja tietokonetilien hallinnointi voidaan hajauttaa tallentamalla ne eri organisaatioyksiköihin (ryhmäkäytännöt).
- Ryhmäkäytännöt periytyvät organisaatioyksiköiden välillä. Ylemmän organisaatioyksikön käytännöt periytyvät alemmalle tasolle. Organisaatioyksikkö voi sisältää toisia organisaatioyksiköitä. Sisäkkäisissä organisaatioyksiköissä ryhmäkäytännöt käsitellään siten, että ylimmän tason käytännöt ensin ja viimeisenä sen tason ryhmäkäytäntöobjektit, mille käyttäjätili kuuluu.
- Toimialueen organisaatioyksiköiden delegointimenetelmien avulla voidaan hallinnointioikeus rajata koskemaan vain tietyn organisaatioyksikön käyttäjätiliä.
- Organisaatioyksiköt parantavat tietoturvaa, koska niiden avulla mahdollistetaan resurssien rajoitettu näkyvyys käyttöoikeusluetteloiden avulla. Käyttäjät pääsevät ja näkevät vain ne tiedot, joihin heillä on oikeus.
- Organisaatioyksiköitä kannattaa luoda, jos halutaan delegoida pienempiä käyttäjäryhmiä ja resursseja koskevia järjestelmähallinnallisia oikeuksia.
- Organisaatioyksiköiden siirto toimialueelta toiselle on mahdollista. (Kivimäki 2005, 370 ja 371.)

Kerran luotu ja hyvin suunniteltu organisaatioyksikkörakenne mahdollistaa uudelleen järjestelyt pienillä objektien siirroilla. Tulevaisuudessa tapahtuvia siirtoja huomioiden kannattaa ottaa huomioon seuraavia seikkoja ennen, kuin luo organisaatioyksiköt:

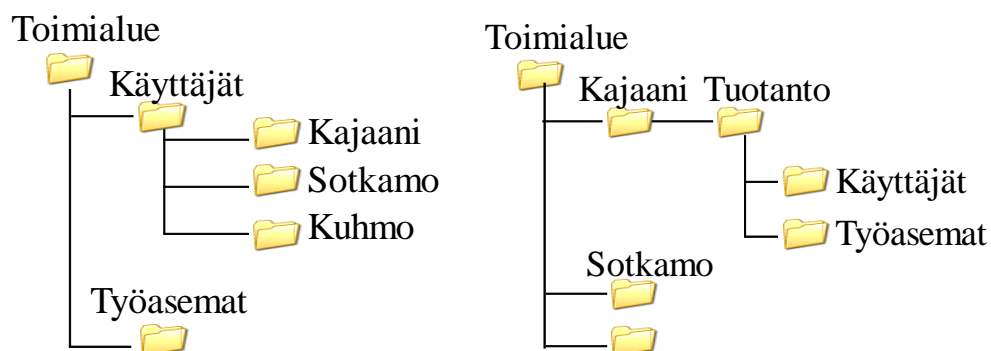
- Rakenteen tulisi mahdollistaa järjestelmänvalvojien tehokas työskentely.
- Organisaatioyksiköiden pitäisi mahdollistaa järjestelmähallinnan delegointi.
- Organisaatioyksiköihin liittyvät käyttöoikeudet.
- Organisaatioyksiköiden avulla voidaan rajoittaa tai laajentaa resurssien näkymistä käyttäjille verkossa.

- Rakenteen pitäisi olla vakaa ja pysyvä.
- Organisaatioyksiköiden sisäkkäisten tasojen määrä ei saisi olla liian monimutkainen. Tasoja saisi olla korkeintaan viisi, mutta yleensä tullaan toimeen korkeintaan kolmella sisäkkäisellä tasolla. (Kivimäki 2005, 372.)

Organisaatorakennetta suunniteltaessa on tärkeää päättää miltä pohjalta hierarkiarakennetta aletaan suunnitella. Liiketoiminta rakennetta heijastavan rakenteen lisäksi voidaan käyttää myös esimerkiksi järjestelmähallintaperusteisia-, maantieteellisiä-, osastokohtaisia- tai projektikohtaisia organisaatioyksiköitä. Alla on havainnollistettu muutamia erilaisia mahdollisia organisaatioyksikkö rakenteita (Kuvio 1 ja 2). (Kivimäki 2005, 372; Partanen 2008.)



Kuvio 1. Järjestelmähallintaperusteinen-, osastokohtainen- ja maantieteellinen organisaatorakenne (Partanen 2008).



Kuvio 2. Hybridimalli organisaatorakenteesta (Partanen 2008).

### 2.3 Toimipaikat

Toimipaikka tai toimipiste (site) määrittää verkon fyysisen rakenteen rajat. ”Toimipaikka muodostuu tietokoneista, jotka ovat yhteydessä toisiinsa LAN -verkon (Local Area Network) välityksellä” (Lintunen 2006, 16).

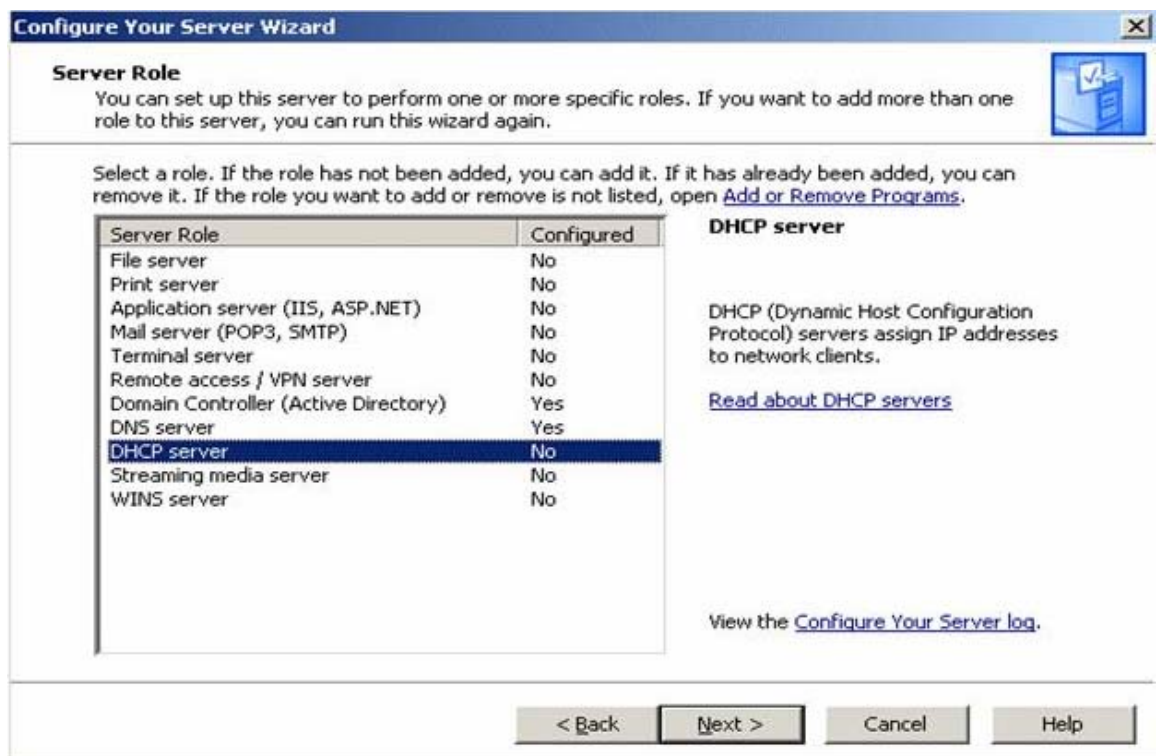
Active Directoryn nimiavaruus ei sisällä toimipaikkoja. Toimipaikka muodostuu yhdestä tai useammasta IP -aliverkosta (Internet Protocol), jotka ovat yhdistetty toisiinsa nopeilla linkeillä. ”Toimipaikan rajat ovat yleensä samat kuin lähiverkon (LAN) tai nopean laajaverkon (WAN) rajat” (Kivimäki 2005, 10). Yleensä Active Directoryn replikointijärjestelmässä toimipaikan sisäinen liikenne on suurempaa kuin toimipaikkojen välinen liikenne. (Kivimäki 2006, 10; Kivimäki 2003, 931.)

Toimipaikkojen vaikutus Active Directoryn toimintaan näkyy seuraavasti: käyttäjän kirjautuessa toimialueelle, Active Directorya käyttävät koneet yrittävät löytää toimialueen ohjauspalvelimen samasta toimipaikasta, jossa käyttäjän työasemakin on. Näin AD:yn kirjautumispyyntöjen käsittely on tehokasta. Käyttäjän etsiessä objekteja Active Directorystä, kuten kirjoittimia, haku ohjataan lähimmälle Global Catalogia (yleinen luettelo) ylläpitävälle ohjauspalvelimelle. Näin myös hakujen käsittely on tehokasta. Toimialueiden välillä tapahtuva Active Directory hakemistojen replikointireitin ja ajan voi konfiguroida. Toimipaikan sisäisessä replikoinnissa ei näin voida tehdä. (Kivimäki 2005, 10.)

### 2.4 Active Directoryn asentaminen ja käyttöönotto

Active Directoryn asentaminen on sama asia kuin palvelimen muuttaminen ohjauspalvelimeksi. Active Directory Installation Wizard eli asennus velho (Kuvio 3) esittää tarpeelliset kysymykset käyttäjälle ja muuttaa sen jälkeen palvelimen ohjauspalvelimeksi luoden Active Directoryn tarvitsemat palvelut sekä käyttämät tietokannat. (Kivimäki 2003, 20.)





Kuvio 3. Manage Your Server Wizard (Microsoft 2008.)

Active Directoryn poistaminen muuttaa ohjauspalvelimen takaisin tavalliseksi palvelimeksi ja tällöin siirrytään käyttämään takaisin palvelimen paikallisia käyttäjätunnuksia (User Account System, UAS). (Kivimäki 2003, 20.)

Ohjauspalvelimen asennuksen yhteydessä tarvitaan seuraavia tietoja:

- Luodaanko uusi toimialue vai lisätäänkö lisäohjauspalvelin jo olemassa olevalle toimialueelle.
- Luodaanko alitoimialue vai uusi puurakenne.
- Liitytäänkö jo olemassa olevaan metsään vai luodaanko uusi metsä. (Kivimäki 2003, 21.)

Asennuksen jälkeen on varmistettava, että asennus on suoritettu onnistuneesti. Asennus on oikein suoritettu käyttöjärjestelmän käynnistyessä normaalisti ja toimialueelle kirjautumisen ollessa mahdollista. Ohjauspalvelimeen asennetut roolit näkee Manage Your Server -sovelluksen kautta. Myös palvelimen tapahtumalokit (Event Viewer) on hyvä tutkia virheti-

lanteiden varalta. Lisäksi asennuksen jälkeen on hyvä tarkistaa toimialueen paikannettavuus ja käsiteltävyys hallintatyökalujen avulla. (Kivimäki 2003, 27.)

## 2.5 Toimialueen hallinta

Active Directoryn hallinnassa tyypillisiä toimenpiteitä ovat:

- toimialueen ja metsän hallinta,
- käyttäjien luonti ja hallinta,
- resurssien julkaiseminen,
- suojausasetusten hallinta,
- organisaatioyksiköiden hallinta,
- delegointi,
- luottosuhteiden hallinta,
- ryhmäkäytännöt,
- tietokonetilien (ja ohjauspalvelinten) hallinta,
- verkkotulostimien hallinta,
- vianselvitys,
- varmistus ja palautus. (Kivimäki 2003, 269; Kivimäki 2005 51.)

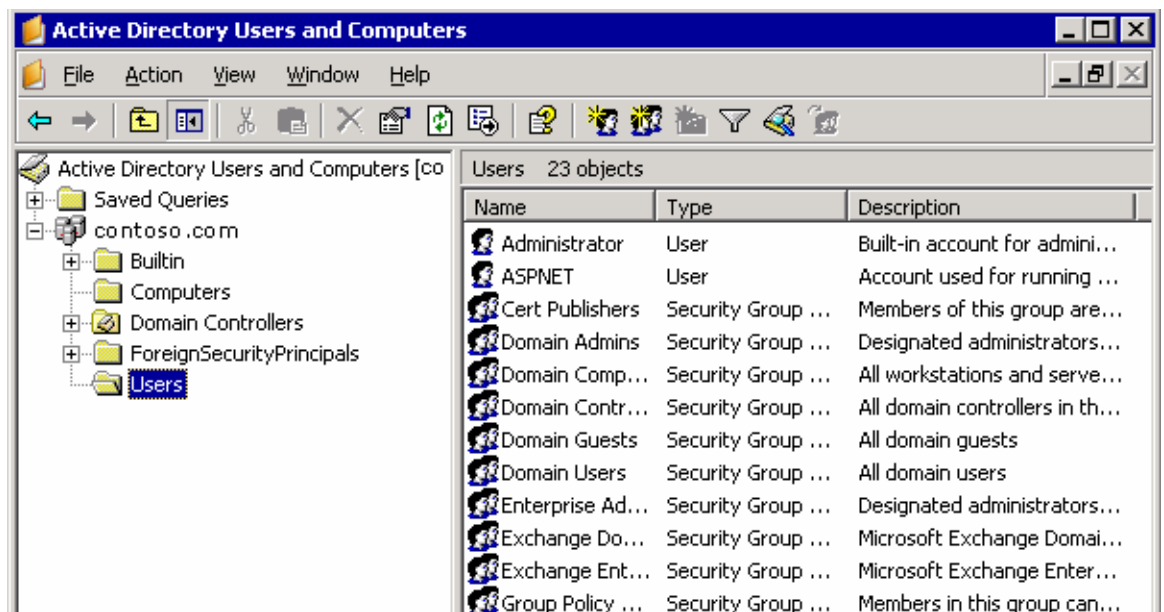
### Toimialueen ja metsän hallinta

Ohjauspalvelimen asennuksen jälkeen Manage Your Server -työkalulla nähdään Active Directoryn toimialueen hallintaan liittyvät tehtävät. Näillä hallintatyökaluilla voi suorittaa useimmat päivittäiset Active Directoryn hallintatoimenpiteet. Nämä hallintakonsolit ovat:

- Users and Computers -hallintakonsoli,
- Domains and Trusts -hallintakonsoli,
- Sites and Services -hallintakonsoli,
- Domain Controller Security Policy -hallintakonsoli,

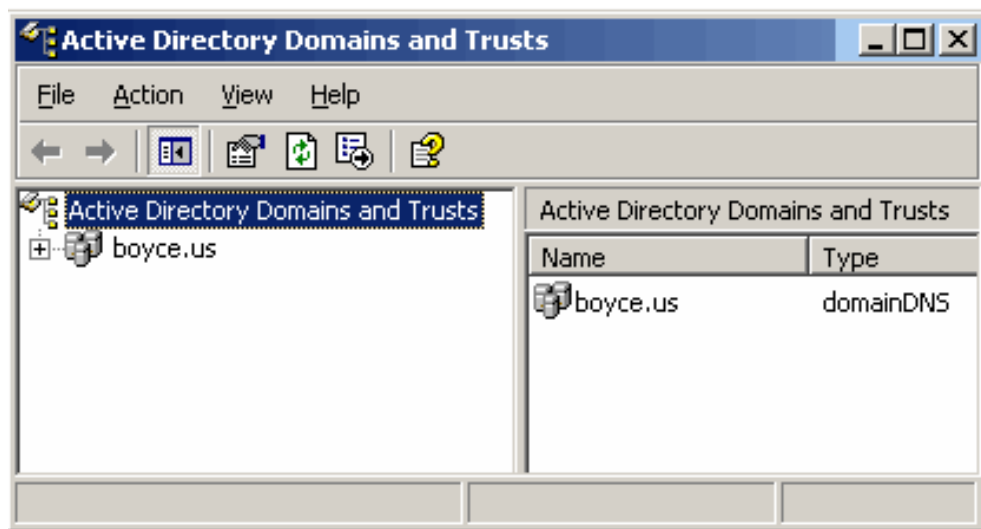
- Domain Security Policy -hallintakonsoli. (Kivimäki 2005, 33-34.)

Users and Computers hallintakonsolilla (Kuvio 4) hallitaan sekä toimialuetta että sen ominaisuuksia, käyttäjiä, ryhmiä, tietokoneita, organisaatioyksiköitä ja ryhmäkäytäntöjä. Myös toimialueen Operations Master -roolien ja toimintatilan hallinta tapahtuu kyseisellä konsolilla. Users and Computers konsolin voi käynnistää myös komentoriviltä komennolla `dsa.msc`. (Kivimäki 2005, 33-34.)



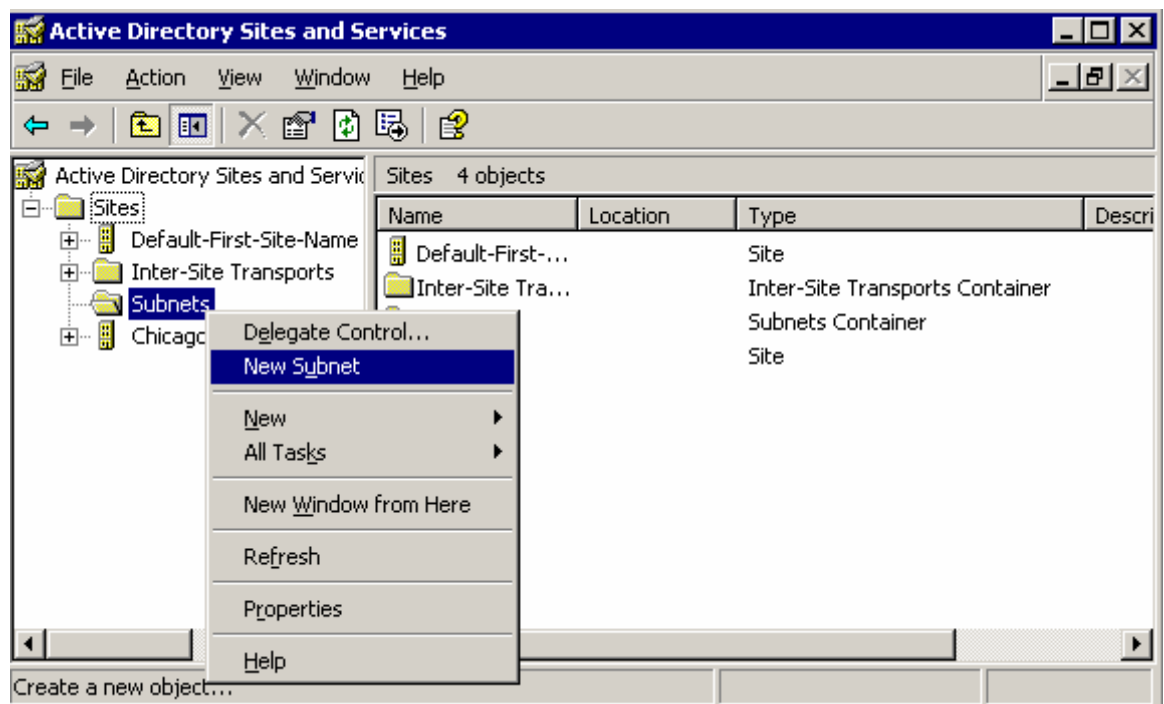
Kuvio 4. Users and Computers -hallintakonsoli (Techrepublic 2004.)

”Domains and Trusts -hallintakonsolin (Kuvio 5) avulla voi hallita toimialueita ja metsiä. Tyypillisiä tehtäviä ovat luottosuhteiden hallinta, toimialueen ja metsän toimintatason asettaminen, kirjautumistunnusten jälkilitteiden (UPN Suffix) lisääminen sekä Domain Naming Mastering -roolin siirtäminen.” (Kivimäki 2005, 33.) Domains and Trusts konsolin voi käynnistää komentorivikomennolla `domain.msc`. (Kivimäki 2005, 33.)



Kuvio 5. Domains and Trusts -hallintakonsoli (Usertify 2008.)

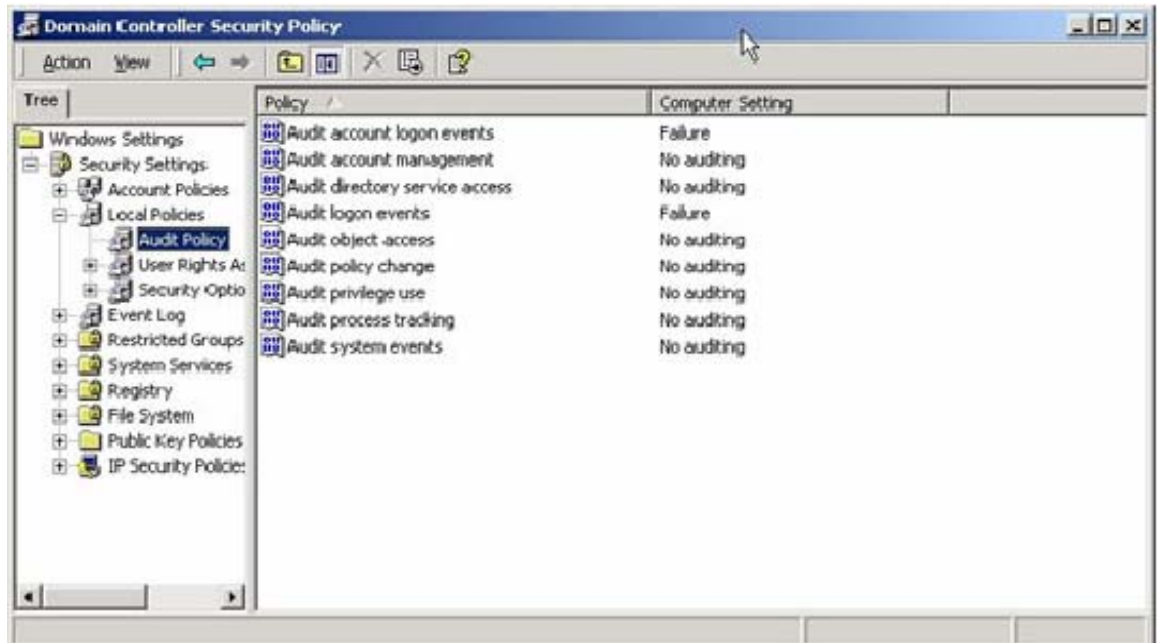
Sites and Services -hallintakonsolissa (Kuvio 6) hallitaan aliverkkoja ja toimipaikkoja palveluineen, myös yleisen luettelon (Global Catalog) määrittely tehdään tällä konsolilla. Tämän konsolin komentokehote on dssite.msc. (Kivimäki 2005, 39.)



Kuvio 6. Sites and Services -hallintakonsoli (SSW 2009.)

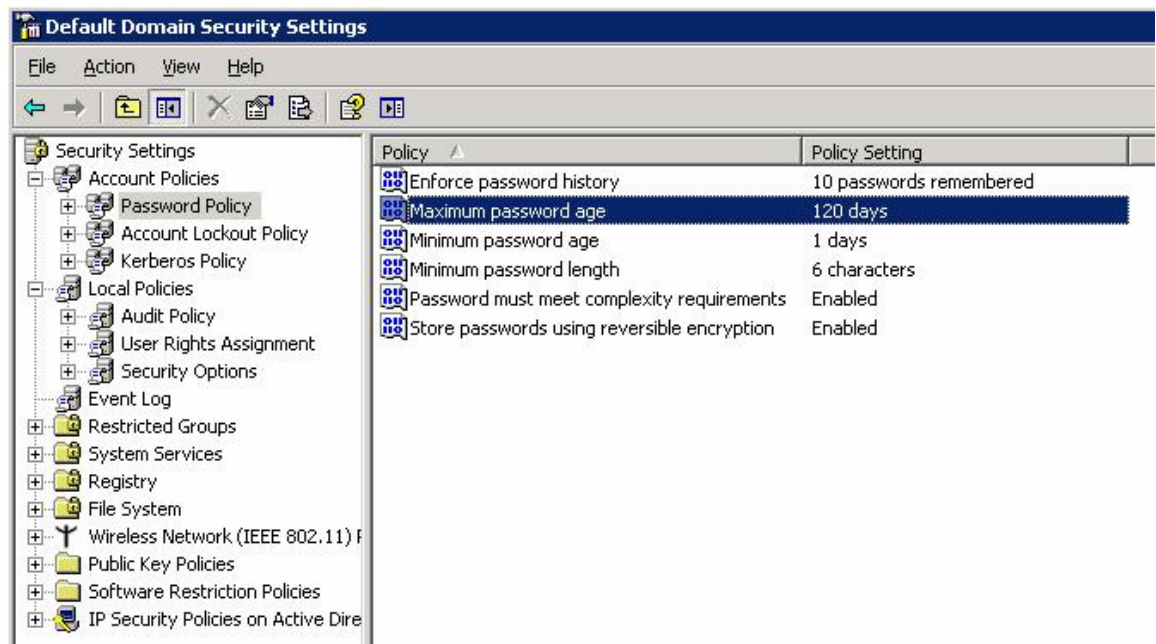
Komentorivikehote dcpol.msc käynnistää Domain Controller Security Policy -hallintakonsolin (Kuvio 7). Tällä hallintakonsolilla hallitaan toimialueen ohjauspalvelinten

suojauskäytäntöjä. Ohjauspalvelinten suojauskäytännöt ovat käytettävissä ainoastaan ohjauspalvelimissa. Default Domain Controller Policy -ryhmäkäytäntö määrittelee toimialueen ohjauspalvelinten suojauskäytännöt. Toimialueelle määritellyt ryhmäkäytännöt ohittavat paikalliset (Local Domain Policy) ryhmäkäytännöt. (Kivimäki 2005, 34 ja 40.)



Kuvio 7. Domain Controller Security Policy -hallintakonsoli (Tools4ever 2009.)

Domain Security Policy -hallintakonsolilla (Kuvio 8) nähdään toimialueen suojauskäytännöt. Ne kohdistuvat toimialueen kaikkiin käyttäjä- ja tietokonetileihin, mutta myös ohjauspalvelimiin sekä jäsenpalvelimiin. Tämäkin hallintakonsoli on käytettävissä vain ohjauspalvelimis- sa. Toimialueen suojauskäytäntöjä ohjaa Default Domain Policy -ryhmäkäytäntö. (Kivimäki 2005, 34 ja 42.)



Kuvio 8. Domain Security Policy -hallintakonsoli (Expert Exchange 2008.)

### Käyttäjien luonti ja hallinta

”Käyttäjätilien hallinnalla tarkoitetaan tilien asetusten muuttamista ja käyttäjäprofiilien sekä kotikansioiden (home directory) määrittämistä.” (Kivimäki 2005, 388.) Kotikansio on käyttäjän henkilökohtainen verkkotallennuspaikka, joka fyysisesti sijaitsee palvelimella. Käyttäjän profiili sisältää käyttäjäkohtaiset työpöytä- ja sovellusasetukset. (Kivimäki 2005, 388.)

Windows 2000/2003 -järjestelmässä on paikallisia ja toimialueen käyttäjätilejä. Toimialueen käyttäjätileillä käyttäjä voi kirjautua toimialueelle käyttäen toimialueen resursseja. Käyttäjätilit määritellään Active Directoryyn Windows 2000/2003 -toimialueissa. Paikallisella käyttäjätilellä voi kirjautua vain tiettyyn koneeseen ja hyödyntää koneen paikallisia resursseja. (Kivimäki 2003, 385.)

Toimialueella on myös valmiiksi luotuja käyttäjätilejä, joilla voidaan suorittaa mm. järjestelmän hallinta tehtäviä (Administrator, järjestelmänvalvoja). Jokaiselle verkon käyttäjälle tulisi kuitenkin luoda oma käyttäjätili, näin käyttäjä pääsee käyttämään toimialueen resursseja. Käyttäjätilit luodaan Active Directory Users and Computers -hallintakonsolilla. (Kivimäki 2005, 388-392.)

Käyttäjätilejä luotaessa on huomioitava seuraavia seikkoja:

- Käyttäjätilien nimeämiskäytännöt: käyttämällä yhdenmukaista nimeämiskäytäntöä käyttäjätilien muistaminen ja etsiminen on helpompaa.
- Sallitut kirjautumisajat: halutaanko käyttäjätilien käyttö estää jonain tiettyinä aikana päivästä tai viikosta. Rajoittamalla kirjautumisaikoja voidaan rajoittaa luvattonta käyttöä.
- Sallitut kirjautumistyöasemat: järjestelmänvalvoja voi määrittää mihin työasemiin käyttäjätilillä voidaan kirjautua. Tehokkain suojaus saadaan, jos käyttäjälle sallitaan kirjautuminen vain omaan työasemaansa. Näin estetään koneilla olevien luottamuksellisten tietojen joutuminen väärin käsiin.
- Käyttäjätilin voimassaoloaika: käyttäjätilille voi määritellä viimeisen mahdollisen käyttöpäivän. Ominaisuuden määrittämisellä voi varmistaa, ettei käyttäjä pääse kirjautumaan verkkoon enää kun hän ei esimerkiksi ole yrityksen palveluksessa.
- Salasanat asetukset: keskeinen menetelmä salasana asetuksia määritellessä on käyttää turvallisia salasanoja. Turvallinen ja tavallinen salasana eroaa siten, että turvallinen salasana on vaikeampi arvata ja murtaa. Active Directory toimialueella on oletuksena käytössä muutamia salasanavaatimus määritelmiä. Asetuksia voi muuttaa Domain Security Policy -hallintakonsolilla.
- Tilien lukituskäytännöt: lukituskäytännöillä voidaan ohjata, koska ja kuinka käyttäjätilit lukittuvat paikallisessa järjestelmässä tai toimialueella. Esimerkiksi tietty määrä väärää salasanoja voidaan asettaa lukitsemaan käyttäjätili.
- Käyttäjäprofiilit: käytetäänkö koneen paikallista profiilia vai palvelimelle tallentuvaa profiilia. Käytettäessä profiilia palvelimelta latautuminen voi hidastaa koneen käynn-

nistymistä. Profiili voidaan myös pakottaa samanlaiseksi tietyille koneille, joka voi sekä helpottaa, mutta myös tietyissä tilanteissa vaikeuttaa järjestelmäylläpitäjän työtä.

- Kotikansiot: luodaanko käyttäjille omat kotikansiot, joihin käyttäjät voivat tallentaa omia henkilökohtaisia tiedostojaan.
- Ryhmäkäytännöt: ne ovat järjestelmän kokoonpanoasetuksia, jotka voidaan liittää Active Directoryn objekteihin kuten organisaatioyksiköihin. (Kivimäki 2005, 404-527.)

### Resurssien julkaiseminen

Resurssien julkaisemisella (Publishing) tarkoitetaan esimerkiksi jaetun kirjoittimen tai jaetun kansion määrittelemistä objektiksi Active Directoryyn. Julkaistu kohde voi sisältää käyttäjille tai järjestelmäylläpitäjille hyödyllisiä tietoja objektista tai se voi sisältää viittauksen jaettuun resurssiin itseensä. Näin käyttäjät voivat käyttää resurssin etsimiseen Active Directoryn haku toimintoa (find). (Kivimäki 2003, 331.)

### Suojausasetusten hallinta

Active Directory -toimialueella suojausasetuksia voidaan määritellä laajemmin kuin yksittäisessä Windows 2000/XP/2003 -tietokoneessa. Toimialueelle tai toimipaikkaan määritellyt suojausasetukset ohittavat aina koneeseen paikallisesti määritellyt (Local Security Settings - asetusten kautta) suojausasetukset. Toimialueen suojausasetuksia voi muuttaa Domain Security Policy - tai Domain Controller Security Policy -hallintakonsolien kautta. (Kivimäki 2005, 129; Kivimäki 2003, 639.)

### Delegointi

Active Directoryn ohjatun toiminnon Delegation of Control avulla voidaan delegoida organisaatioyksikön hallintatehtäviä. Delegointi tapahtuu käytännössä liittämällä objektiin käyttöoikeuksia. Nämä oikeudet antavat käyttäjien tai ryhmien tehdä hallintatehtäviä, kuten luoda tai muuttaa organisaatioyksikön objekteja. Tehtävien delegointi mahdollistaa järjestelmänhallinnan hajauttamisen. Näin pystytään säästämään rahaa ja aikaa järjestelmänhallinnassa. (Kivimäki 2005, 377; Kivimäki 2003, 363.)



## Luottosuhteet

Luottosuhteet yhdistävät toimialueita ja mahdollistavat samalla tiedonsiirron toimialueiden välillä luotettavasti (Secure Channel). Luottosuhde sallii luotettavan toimialueen käyttäjien päästä käyttämään luotetun toimialueen resursseja. Tämä mahdollistaa myös eri toimialueille luodun käyttäjän kirjautumisen toisen toimipaikan koneeseen ilman, että toiselle toimialueelle tarvitsee luoda käyttäjälle tunnusta. (Kivimäki 2005, 6; Kivimäki 2003, 981.)

## Ryhmäkäytännöt

Ryhmäkäytäntö on mekanismi, jolla hallitaan koneiden asetuksia Active Directory -toimialueella. Ryhmäkäytännöt ovat tulleet käyttöön Windows 2000 -käyttöjärjestelmän myötä. Ryhmäkäytännöt ovat sääntöjä, jotka auttavat järjestelmänylläpitäjää hallitsemaan käyttäjiä ja tietokoneita. Käytäntöjen avulla voidaan hallita käyttäjien ympäristöasetuksia, ohjelmien jakeluasetuksia, salasanaikäytäntöjä ja monia muita asetuksia. Windows Server 2003 -käyttöjärjestelmässä ryhmäkäytäntöjen hallintaa ja toteuttamista on helpotettu mutta perusteita ei ole varsinaisesti muutettu. (Kivimäki 2005, 527.)

Ryhmäkäytännöt ovat objekteja (GPO, Group Policy Objects), joihin asetukset tallennetaan. Ryhmäkäytännöt ovat toiminnassa vain Windows 2000 - ja uudemmissa käyttöjärjestelmissä. Ryhmäkäytäntöasetukset on jaettu käyttäjiin ja koneisiin liittyviin asetuksiin. Käytännössä ryhmäkäytäntöasetukset päivittyvät käyttäjän koneelle hänen kirjautuessa järjestelmään tai ulos järjestelmästä, mutta myös järjestelmää käynnistäessä tai sammuttaessa. (Kivimäki 2005, 527; Stanek 2003, 86 - 87.)

## Tietokonetilien hallinta

Tietokonetilejä luodaan ja hallitaan Active Directory Users and Computers -hallintakonsolilla. Tietokonetili voidaan luoda joko liittämällä tietokone suoraan Active Directory -verkkoon eli toimialueeseen tai luomalla tietokonetili etukäteen Users and Computers -konsolilla. (Stanek 2003, 162 - 163.)

## Verkkotulostimet

Verkkotulostimet julkaiseminen Active Directoryyn tapahtuu asentamalla kirjoitin ensin palvelimelle tavalliseksi kirjoittimeksi. Tämän jälkeen kirjoittimen ominaisuuksien kautta kirjoitin julkaistaan Active Directory -objektina. Kirjoittimen julkaiseminen jälkeen käyttäjä voi hakea kirjoitinta työasemansa find -toimintoa käyttäen. Verkkotulostinten käyttö helpottaa kirjoittimien asentamista käyttäjien työasemille.

### 3 JÄRJESTELMÄN YLLÄPITO

Järjestelmän ylläpito koostuu useista osa-alueista. Näitä ovat esimerkiksi käyttäjätuki, verkonhallinta tehtävät ja palvelinten ylläpito ja nykyisin yhä suuremmissa määrin järjestelmän tietoturvallisuudesta huolehtiminen ja ongelmien ennaltaehkäisy. Pienissä organisaatioissa järjestelmän ylläpito on usein toteutettu ulkopuolisen yrityksen toimesta. Suuret organisaatiot taas mahdollistavat oman mikrotuen käytön. Suurissa organisaatioissa on myös mahdollista jakaa ylläpitotehtävät siten, että jokaisella järjestelmän ylläpitäjällä on oma erikoisalansa. (Anttonen & Kilpeläinen 2007, 4; Oulun yliopisto 2000.)

Verkonhallinta tehtävät koostuvat toimivien verkkoyhteyksien hallinnasta ja luomisesta. Tähän kuuluu mm. työasemien liittäminen verkkoon, verkkolaitteiden asennus ja ylläpito sekä verkkoratkaisujen suunnittelu ja käyttöönotto. Tällainen verkkoratkaisu voi olla myös Active Directory -verkon suunnittelu ja käyttöönotto.

Järjestelmän ylläpitotehtäviin kuuluu mm. käyttäjätuki, joka käsittää työasemien asentamisen, päivittämisen, uusien ohjelmistojen asennuksen sekä vanhojen päivittämisen, mutta myös käyttäjien ongelmien ratkaisemisen. Nykyisin käyttäjätuki voidaan hoitaa myös Help Desk -ratkaisulla, joka tarkoittaa keskitettyä palvelua johon käyttäjät ilmoittavat kaikki tietokoneisiin liittyvät ongelmat.

Järjestelmän ylläpitoon kuuluu suurena osana myös asioiden dokumentointi. Hyvällä dokumentoinnilla varmistetaan ratkaisun löytyminen vastaisuuden varalle. Samalla tavalla, kun pidetään kirjaa tehdyistä töistä, dokumentoidaan myös lisenssit, käyttäjätunnukset ja koneet sekä esimerkiksi jokaiselle koneelle asennetut ohjelmat.

#### 3.1 Active Directory järjestelmäylläpidossa

Järjestelmäylläpidossa Active Directory on todella hyödyllinen. Active Directoryn avulla fyysisesti eripaikoissa ja paikkakunnillakin sijaitsevia resursseja voi hallinnoida yhdestä paikasta. Tämä helpottaa järjestelmäylläpitäjän työtä. Samalla organisaatiossa voidaan säästää kuluissa kun järjestelmäylläpitäjän ei tarvitse välttämättä matkustaa toiselle paikkakunnalle.

Active Directory mahdollistaa resurssien hallinnan jakamisen. Tämä tarkoittaa sitä että Active Directoryssä voidaan antaa esimerkiksi yhdelle käyttäjälle oikeudet hallinnoida tietyn organisaation tai ryhmän oikeuksia. Tämän ominaisuuden avulla organisaatiossa voidaan jakaa tiettyjen objektien hallinnointitehtävät yksilöllisemmin. Tämä taas vähentää järjestelmäylläpitäjän työtaakkaa.

Ryhmäkäytäntöjen avulla käyttäjien työasemille voi pakottaa tiettyjä asetuksia. Käytäntöjen avulla voi varmistaa ettei käyttäjä pääse tekemään sellaisia toimintoja jotka voivat vaikuttaa työaseman toimintaan. Asetuksia ovat esimerkiksi start -valikosta ohjaspaneelin piilottaminen tai työasemalla käytössä olevan teeman pakottaminen tietynlaiseksi kaikilla yrityksen koneilla.

Kuten yllä mainitut Active Directoryn ominaisuudet myös muut toiminnot helpottavat ja samalla yksinkertaistavat ylläpitäjän työtä. Tämä kuitenkin vaatii hyvän suunnittelun ennen toteutusta. Tätä kautta järjestelmäylläpito helpottuu eikä vaadi järeitä muutostöitä Active Directoryn käyttöönoton jälkeen.

#### 4 MONDO MINERALS B.V.

Mondo Minerals B.V. on johtava innovatiivisten ja korkealaatuisten talkkituotteiden valmistaja, jonka tuotteet on suunniteltu tuottamaan lisäarvoa maali-, muovi- ja paperi- sekä monille muille teollisuuden tuotteille. Mondo Minerals on maailman toiseksi suurin talkkituotteiden valmistaja noin 15 prosentin markkinaosuudella. Yrityksen toiminta on keskittynyt Keski- ja Pohjois-Eurooppaan, missä sillä on vahva asema paperimarkkinoilla. (Mondo 2008.)

Yritys on perustettu vuonna 1967 Suomen Talkki Oy: nimellä ja tuotanto alkoi paria vuotta myöhemmin. Tuolloin yhtiön tuotantokapasiteetti oli 70 000 tonnia vuodessa, mutta nykyisin yhtiön kokonaistuotantokapasiteetti on noin 650 000 tonnia vuodessa. Puolet koko yhtiön tuotannosta menee vientiin. (Piipponen 2008.)

Mondo Mineralsilla on tuotantolaitoksia neljällä paikkakunnalla: Sotkamossa, Vuonoksessa sekä kaksi Hollannissa. Suomessa sijaitsevat tuotantolaitokset toimivat Mondo Minerals B.V. Branch Finland -nimikkeen alla. Suomessa yrityksellä on kahden tuotantolaitoksen lisäksi myös konttori Helsingissä. Sotkamon tehdas on maailman suurin talkkitehdas. Yrityksen palveluksessa työskentelee yhteensä noin 170 henkeä. Liikevaihto oli vuonna 2007 noin 111 miljoonaa euroa. (Piipponen 2008; Mondo 2008.)

Mondo Minerals Oy on ollut vuodesta 2001 alkaen sveitsiläisen perheyrityksen omistama. Hg Capital osti yrityksen 31.10.2008. Yhtiö fuusioitui 31.7.2008 hollannissa olevaan yhtiöön Mondo B.V. ja tämän myötä Suomen yhtiöstä tuli Mondo Minerals B.V. Branch Finland. (Piipponen 2008.)

##### 4.1 ATK -organisaatio

Mondo Mineralsin atk-organisaatiossa työskentelevät tietohallintopäällikkö ja mikrotukihenkilö. Järjestelmänylläpitäjillä on noin 150 työasemaa hallittavana kolmella paikkakunnalla Suomessa.

Suurin osa työasemista ja palvelimista sijaitsee Sotkamossa, Korholanmäen tehtaalla, noin 100 työasemaa ja 20 palvelinta. Loput yrityksen käytössä olevista palvelimista ja työasemista

sijaitsevat Vuonoksessa ja Helsingissä. Lisäksi yrityksen järjestelmänylläpitäjillä on ylläpidettävään muutamia tuotantokäytössä olevia työasemia, joilla varmistetaan tuotteiden laadullisia ominaisuuksia.

Mondo Mineralsin käytössä ei ole Help Desk -palvelua vaan käyttäjätuki hoidetaan sähköpostin ja puhelimen välityksellä. Usein käyttäjät saattavat kysyä ratkaisua ongelmiinsa myös suoraan järjestelmänylläpitäjältä henkilökohtaisesti. Tämä toimintatapa on ollut Mondolle sopivin mahdollinen ratkaisu. Järjestelmänylläpitäjien työtehtävät koostuvat käyttäjien auttamisen lisäksi mm. uusien koneiden asentamisesta, palvelinten ylläpidosta sekä muiden juoksevien asioiden hoitamisesta.

## 5 ACTIVE DIRECTORYN TOTEUTUS MONDO MINERALSILLE

Mondo Minerals Oy suunnitteli jo vuonna 2006 ensimmäisen kerran uuteen Microsoftin Active Directory -verkkoon siirtymistä. Tuolloin verkkouudistukseen ei kuitenkaan ollut resursseja, joten toteutus siirtyi tulevaisuuteen.

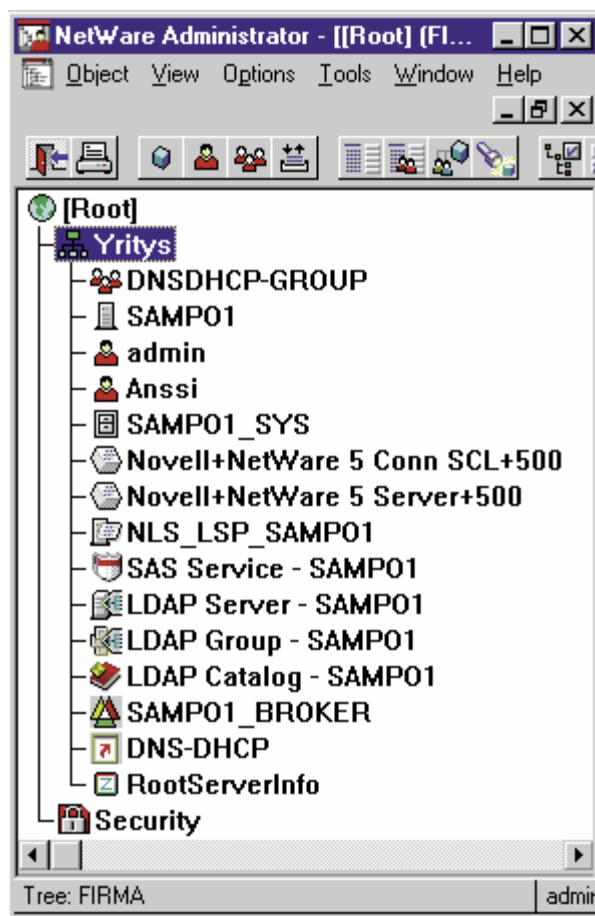
Vuoden 2007 lopussa Active Directoryn käyttöönotto tuli ajankohtaiseksi yrityksessä tapahtuneiden hallinnallisten muutosten vuoksi. Tuolloin projektille löytyi aikaa, resursseja ja toteuttaja. Active Directory haluttiin ottaa käyttöön, koska silloinen yrityksen omistaja Omya Ag halusi näin tehtävän. Näin siis tuolloin käytössä olleesta Novell Netwaresta ei edes kartoitettu uudemman version mahdollista käyttöönottoa.

Uuteen verkkojärjestelmään siirtymisen etuna oli myös se, että upouuden järjestelmän ansiosta kaikkia ylimääräisiä, vuosien saatossa luotuja, käyttämättömiksi jääneitä ryhmiä ja käyttäjätilejä ei tarvinnut siirtää uuteen verkkoon, vaan ne poistettiin. Näin verkon rakenne selkeytyi.

Active Directory -projekti alkoi vuoden 2008 alussa, jolloin Active Directoryn hahmottelu alkoi. Heti projektin alkuun yritykseen investoitiin uusi virtuaalipalvelin, johon asennettiin Active Directory ja sen tarvitsemat palvelut. Näin myös yrityksen palvelinkanta päivittyi. Palvelinten virtualisointi helpotti useiden aiemmin erillisten palvelinten hallintaa.

Projektin alussa palvelimien konfiguroinnin ja Active Directoryn asennuksen hoiti CitiusNet -yritys. CitiusNet toimi myös asiantuntijana ja apuna ongelmissa, joita Active Directoryn myötä ilmeni. Myös Jyrki Kivimäen kirjoittama Active Directory- kirjallisuus tuki projektin aikana.

Ennen Active Directory -verkkoa Mondo Mineralsilla oli käytössä Novell Netware -verkkopalvelu (Kuvio 9). Netware on Novellin ratkaisu verkkopalvelusta vastaava kuin Active Directory Microsoftilla. Netwarella käyttöliittymä on vanhanaikaisen näköinen verrattuna Active Directoryyn. Osaltaan tämä johtuu siitäkin, että Active Directoryn käyttöliittymä on Microsoftin tekemä ja näin ollen samantyyppinen kuin Microsoftin muilla tuotteilla (esimerkiksi Microsoft XP - ja Microsoft Server -käyttöjärjestelmät). Microsoftin tuotteet ovat käyttäjille yleensä tutumpia kuin muiden tietotekniikka-alan yritysten.

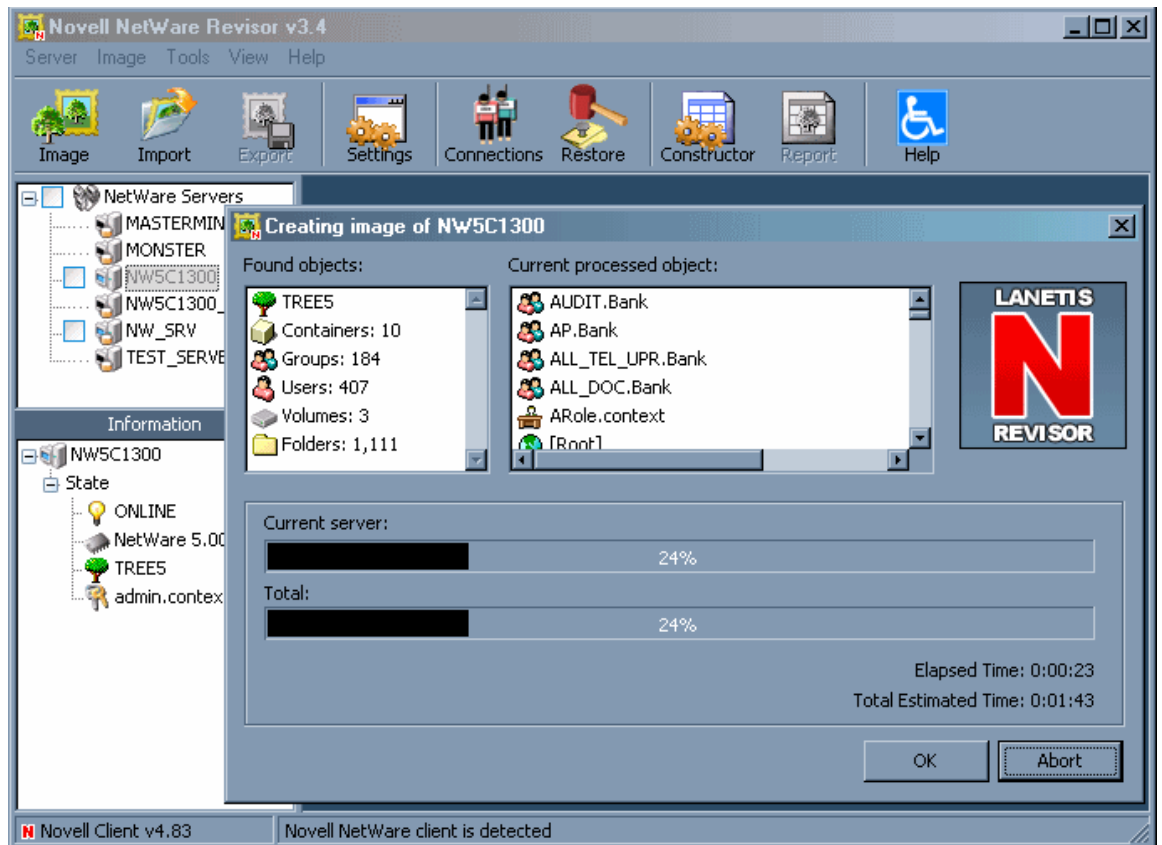


Kuvio 9. Näkymä Novell NetWare -ohjelman hallintakäyttöliittymästä. (Tietokone.fi 2007.)

Projekti käynnistettiin kartoittamalla Novellissa tuolloin olleet tiedot. Novell Netware Revisor -ohjelma ajoi listat vanhan verkon käyttäjistä, ryhmistä ja jaetuista kansioista sekä eri paikkakuntien verkkojen rakenteista. Näiden listojen avulla saatiin suuntaa-antava käsitys tarvittavista ryhmistä ja käyttäjistä, jotka tulisi luoda uuteen verkkopalveluun.

Netware Revisor (Kuvio 10) on Novellin tarjoama ohjelma, jolla voi hallita Netware -verkkoa. Ohjelmalla voidaan ajaa myös erilaisia listoja jo olemassa olevasta Netware -verkon rakenteesta, kuten tässä projektissa. Mondo Mineralsilla ohjelmaa ei ole käytetty Netwaren hallintaan vaan ainoastaan verkkorakenteen listaamiseen Active Directory -projektin aikana.





Kuvio 10. Novell NetWare Revisor 3.4 -ohjelman käyttöliittymä (Topsofts 2008.)

Vuonna 2006 tehdyssä selvityksessä Atk -osaston henkilökunta kävi läpi kunkin osaston henkilökunnan kanssa heidän verkkohakemistonsa. Näin siis projektin uudelleen käynnistymisen yhteydessä tulevan verkon rakenteesta oli jo jonkinlainen käsitys. Kartoituksessa oli käyty läpi käyttäjien kanssa hakemistot siten, että tiedettiin, mitkä hakemistot oli tarkoitus siirtää uuteen verkkoon ja mitkä tiedot jätettäisiin Novelliin tai siirrettäisiin arkistoitavaksi. Tuolloin oli myös hahmoteltu verkkohakemistojen mahdollisia kirjaimia.

Nimeämiskäytännöt suunniteltiin yhdessä henkilökunnan kanssa siten, että niistä saatiin selkeät ja yhdenmukaiset. Samalla päätettiin periaatteet, joiden mukaisesti uutta verkkoa alettaisiin hahmotella. Tässä vaiheessa päätettiin mm. verkon organisaatioyksikkörakenteista, kaikkien verkkoon sijoitettavien objektien nimeämiskäytännöistä sekä ryhmien nimeämiskäytännöistä. Rakennettaessa uutta verkkoa verkkorakenne selkeytyi todella paljon. Entisessä Novell -verkossa oikeuksia oli annettu käyttäjille jopa liikaa, joten uuteen verkkoon siirryttäessä myös oikeus asioita harkittiin tarkkaan.

Hyvän ja kattavan suunnittelun jälkeen siirryttiin testaamaan Active Directoryä käytännössä. Testaus suoritettiin aluksi liittämällä muutamia testikoneita Active Directoryyn ja testaamalla erilaisia käyttäjätilien asetuksia ja oikeuksia verkossa. Testaus suoritettiin lisäämällä ja poistamalla oikeuksia, jolloin nähtiin kuinka asetukset vaikuttavat käyttäjän oikeuksiin. Samalla päätettiin, että käyttäjillä olisi täydet oikeudet työasemillensa ja oikeuksia rajoitetaan vain verkon kautta. Tämä tapa tuntui projektin alussa parhaalta vaihtoehdolta myös sen vuoksi, että käyttäjät olivat tottuneet muuttamaan mm. profiiliasetuksia koneillansa (esimerkiksi työaseman näytöllä olevaa taustakuva).

Active Directoryn mahdollistamaa palvelimelta latautuvaa profiili -ominaisuutta ei otettu käyttöön, kuitenkin myös tämä ominaisuus testattiin ennen kuin tehtiin lopullinen päätös käyttämättä jättämisestä. Lopputulokseen päädyttiin sen vuoksi, että käyttäjät käyttävät pääasiassa vain omaa työasemaansa. Näin ollen käyttäjää seuraavalla profiililla ei käytännössä olisi ollut suurta hyötyä. Ominaisuuden käyttöönotto olisi luultavasti ainoastaan hidastanut työaseman avautumista, latautuessaan palvelimelta.

## 5.1 Active Directoryn käyttöönotto

Käyttäjien liittäminen Active Directory -verkkoon alkoi keväällä 2008. Ennen käyttäjien liittämistä Active Directoryyn täytyi palvelimelle luoda käyttäjätilit. Jokaiselle käyttäjälle luotiin oma käyttäjätunnus. Käyttäjätunnuksen luonnin yhteydessä käyttäjälle määriteltiin myös oma kotihakemisto, joka toimii henkilökohtaisena verkkoasemana.

Kotihakemisto on Active Directory -palvelimella fyysisesti sijaitseva kansio, joka on jaettu näkymään käyttäjän koneella resurssienhallinnassa. Käyttäjä voi käyttää kotihakemistoaan esimerkiksi omien henkilökohtaisten töidensä tallettamiseen. Kotihakemisto on parempi paikka tallettaa tiedostoja, kuin työaseman levyasemat, koska palvelimella oleva hakemisto varmistetaan joka päivä. Näin siis esimerkiksi työaseman rikkoutuessa käyttäjän tiedostot ovat tallessa palvelimella. Kriittisimmistä koneista tehtiin kuitenkin vielä varmuuskopiot ennen, kuin ne siirrettiin Active Directory -verkon palveluja käyttämään. Kuitenkaan kaikista koneista ei tehty varmistusta ennen siirtoa, koska se olisi vienyt liian paljon aikaa.

Käyttäjien luomisen jälkeen suunniteltiin käyttäjäryhmät ja päätasot verkkohakemistoista sekä luottiin ryhmät ja hakemistot Active Directory -palvelimelle. Hakemistojen ja ryhmien

luomisen jälkeen käyttäjät liitettiin ryhmiin, joiden kautta oikeudet verkossa määrittyvät. Käyttäjän kirjautuessa verkkoon hän pääsee ainoastaan niihin verkkohakemistoihin, joihin hänellä on oikeus.

Tarvittaessa käyttäjälle voidaan lisätä oikeuksia, mutta tarvittaessa myös oikeuksien poistaminen on mahdollista. Harvoin käyttäjä kertoo järjestelmänylläpitäjälle, jos hänellä on liikaa oikeuksia. Näin ollen oikeuksien tarvittavan määrän antaminen on suunniteltava hyvin, ettei käyttäjä pääse käsiksi tiedostoihin, joita hänen ei pitäisi nähdä. Tällaisia tiedostoja voivat olla esimerkiksi henkilöstöhallinnon palkkatiedot.

Ennen käyttäjien koneiden liittämistä Active Directory -verkkoon tiedotettiin heille käyttöönotettavan verkon päätoimintaperiaatteista. Tiedotteessa kerrottiin esimerkiksi näkymän muuttumisesta resurssien hallinnassa ja pahoiteltiin mahdollisia käyttökatkoksia. Tiedottamisen sekä oikeuksien asettamisen ja testaamisen jälkeen käyttäjän työasema liitettiin uuteen Active Directory -verkkoon. Koneen liittäminen verkkoon tehdään käyttäjän koneella, joten käyttäjä ei voi kyseisenä aikana käyttää työasemaansa.

Active Directory -verkkoon siirtyminen Mondo Mineralsilla toteutettiin vaiheistetusti kaikilla paikkakunnilla eri aikaan. Verkkoon siirtyminen aloitettiin kopioimalla tiedostot Novell -palvelimelta Active Directory -palvelimelle. Samalla käyttäjän kone liitettiin Active Directoryyn. Osa tiedostojen siirrosta palvelimelta toiselle suoritettiin illalla, jotta käyttäjät eivät kärsisi käyttökatkoksista, mutta kuitenkin osa tiedostoista täytyi siirtää päivällä, josta aiheutui käyttökatkoksia.

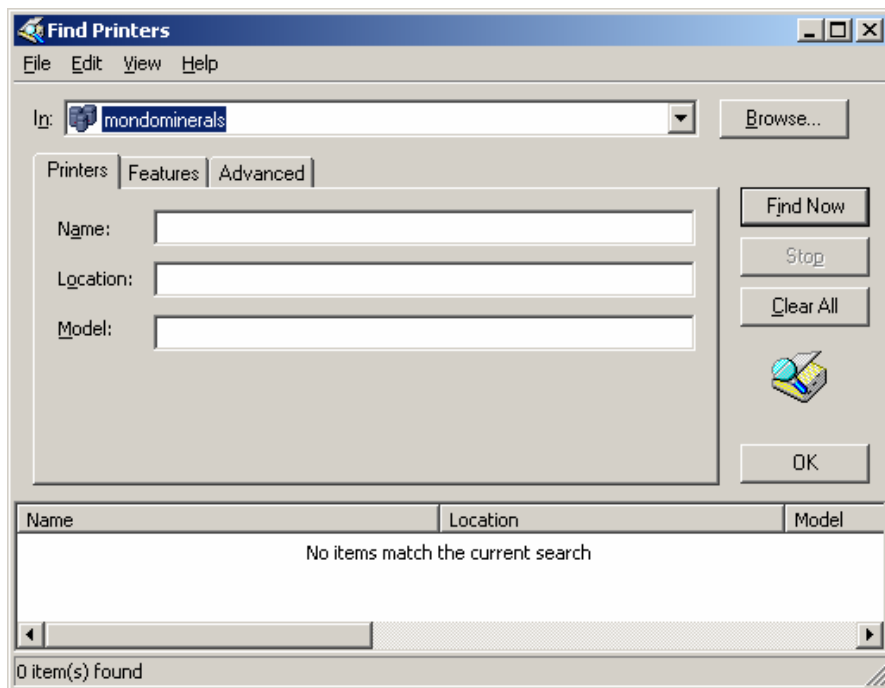
Helsingin verkon käyttäjien siirtämiseen ensimmäisenä päädyttiin, koska yrityksen henkilökunnasta pienin osa työskentelee Helsingissä. Siirtyminen pyrittiin aloittamaan ”helpoimmas- ta” paikkakunnasta. Helsingin siirtyminen toteutettiin siten, että yksi ATK -organisaation työntekijöistä lähti paikanpäälle Helsinkiin ja kaksi muuta henkilöä jäi Sotkamoon työasemiensa ääreen luomaan käyttäjille salasanoja ja siirtämään käyttäjien tiedostoja Novell -verkosta Active Directory -verkkoon.

Tiedostojen siirtäminen palvelimelta toiselle toteutettiin siten, että järjestelmänylläpitäjien koneet liitettiin Active Directory -verkkoon. Active Directory -verkon rinnalla toimi myös Netware -verkko. Tämä siis mahdollisti kahden palvelimen resurssien käytön samanaikaisesti. Myös etäyhteys työasemien välillä tai palvelimen ja työaseman välillä oli aika-ajoin käytös-

sä. Siirtymä vaiheessa Novell -verkko oli koko ajan käyttökelpoinen, joten Novell olisi voitu ottaa uudestaan käyttöön, mikäli siirtymä aikana olisi ilmennyt isoja ongelmia Active Directoryn kanssa.

Helsingin jälkeen siirrettiin Vuonos ja viimeisenä Sotkamo. Vuonoksessa ja Sotkamossa oli muutamia tuotantokäytössä olevia työasemia, joihin on liitetty räätälöityjä ohjelmia sekä mittalaitteita. Näitä työasemia käytetään talkkituotteiden laadullisten ominaisuuksien tarkkailuun. Kyseisten työasemien liittäminen Active Directory -verkkoon oli haasteellisinta, sen vuoksi että työasemat täytyi saada toimimaan virheettömästi mahdollisimman lyhyen ajan kuluessa, jotta niillä voitiin jatkaa tuotteiden laadun tarkkailua. Muutama työasema liitettiin takaisin Novelliin ennen kuin Active Directory -verkossa koneiden toiminta varmistui. Näihin mittalaitteisiin jouduttiin pyytämään ohjelmallisia muutoksia ohjelmien toimittajilta, että koneet saatiin liitettyä Active Directory -verkkoon ja toimimaan oikein.

Kirjoittimet julkaistiin myös Active Directory -verkossa. Kirjoittimien julkaiseminen helpottaa kirjoittimen asentamista käyttäjän työasemalla. Kirjoittimien Active Directoryyn julkaisemisen myötä ylläpitäjän on helppo asentaa kirjoitin käyttäjän koneelle find -toiminto (Kuvio 11) käyttäen. Verkkotulostinten etsintä mahdollistaa myös käyttäjien omatoimisen verkkotulostinten etsimisen Active Directorystä.



Kuvio 11. Find Printers -toiminto.

Käyttäjien työasemien siirtäminen Active Directory -verkkoon kesti suhteellisen kauan, koska jokainen työasema täytyi käydä läpi yksitellen. Kunkin työaseman liittämisessä Active Directoryyn meni tunnista kahteen tuntiin aikaa. Joidenkin koneiden kanssa meni enemmän ja muutama kone asennettiin jopa uudestaan, että kaikki ohjelmat alkoivat toimia oikein. Koneen Active Directory -verkkoon siirtämisen jälkeen työasemista tehtiin vielä varmuuskopioita. Näin saatiin päivitettyä yrityksen käytössä oleva laaja image -varasto Active Directory aikaan.

## 5.2 Dokumentointi

Mondo Mineralsilla Active Directoryn ryhmien, käyttäjätilien ja verkkojakojen dokumentointi hoidettiin Excel taulukon (Kuvio 12) avulla. Taulukossa on kolme välilehteä, johon yhteen laitettiin käyttäjäryhmät, toiseen verkkojaot ja kolmannelle välilehdelle kirjattiin kaikki käyttäjät. Taulukon avulla voidaan pitää kirjaa mihin kullakin käyttäjällä oli oikeuksia. Verkkojaot välilehdellä oli allekkain kaikki jaetut verkkohakemistot ja niiden alla olleet pääkansiot. Yläriiville kirjattiin ryhmät ja merkittiin rastilla ja värejä käyttäen millä ryhmällä on oikeus mihinkin kansioon. Värillä kerroivat taulukossa oikeuksien periytymisestä.

	Deny	D					
	Full control	F					
	Special (ei poistamista)	S					
	Read & Execute	E					
	Read	R					
	Write	W					
	List	L					
	Modify	M					
	Koko nimi	DL_SMO_HR	DL_SMO_MANAGEMENT_GROUP	DL_SMO_MINING	DL_SMO_MINING_TRAINERS	DL_SMO_MAINTENANCE	
Jako:	Data	F					
	\						
	Heha	F					
	IT	F					
	Johtoryhmä		F				
	Kaivos			F			

Kuvio 12. Ote oikeudet -taulukosta.

Alkuun dokumentoitiin siten, että jokaisella paikkakunnalla (Sotkamo, Vuonos ja Helsinki) oli omat asiakirjat. Myöhemmin huomattiin, ettei kannata säilyttää Helsinkiä ja Vuonosta erillisissä taulukoissa, koska osalla toisen paikkakunnan käyttäjistä täytyi olla oikeuksia esimerkiksi Sotkamon verkkojakoihin. Näin muutettiin dokumentointi järjestelmää siten, että kaikkien paikkakuntien tiedot koottiin yhteen asiakirjaan.

### 5.3 Case -projektin yhteenveto

Active Directory -verkko projekti kesti kokonaisuudessaan vuodesta 2006 vuoteen 2008. Vuoden 2006 aikana yrityksen mikrotukihenkilöt tekivät esiselvityksen Active Directoryn käyttöönotolle. Kyseisenä aikana oli kartoitettu organisaatioiden verkkohakemistot ja samalla hahmoteltu tulevia, mahdollisia verkkohakemistojen kirjaimia. Projekti jäi odottamaan tekijää vuoden 2007 loppuun. Tuolloin Active Directoryn suunnittelu alkoi. Kevään 2008 aikana Active Directory -verkko alkoi hahmottua ja kesällä 2008 Mondo Minerals B.V. Branch Finlandin käytössä oli Active Directory -verkkopalvelu.

Projektin aikana ilmeni suhteellisen vähän ongelmia. Suurimmat ongelmat ilmaantuivat tuotantokäytössä olevien työasemien siirrossa Active Directoryyn. Työasemissa olleet mittausohjelmat eivät nimittäin toimineet oikein siirron jälkeen. Suunnittelun yhteydessä tehdyn varasuunnitelman ansiosta työasemat oli kuitenkin mahdollista liittää takaisin käyttämään vanhan Novelliin palveluja. Mittaustyöasemien kanssa ilmenneet ongelmat saatiin ratkaistua pyytämällä ohjelmallista muutosta sovellusentomittajalta.

Profiilisiirrot tuottivat testauksen aikana ongelmia. Ongelma selvitettiin päättämällä olla käyttämättä profiilisiirtoa. Tämä kuitenkin hidasti käyttäjän koneen liittämistä Active Directoryyn; työpöydällä olleiden pikakuvakkeiden hakeminen oli aikaa vievää ja toisinaan myös turhauttavaa työasemilla joilla oli paljon pikakuvakkeita. Testauksen yhteydessä todettiin kuitenkin, ettei profiilisiirrosta ole hyötyä käyttäjälle, joten ominaisuutta ei otettu käyttöön.

Netwaren aikana toisen paikkakunnan verkkohakemistoihin pääsy oli hidasta. Active Directoryn myötä myös paikkakuntien väliset linkit toimivat nopeammin. Tämä helpotti sekä hosti käyttäjien päivittäistä työskentelyä.

Projektin alussa yrityksen työntekijöille tiedotettiin Active Directory -projektista. Näin käyttäjät olivat tietoisia tulevista muutoksista. Käyttäjät omaksuivat nopeasti uudet toimintatavat. Suurinta hämmennystä käyttäjien keskuudessa herätti yhteisen verkkoaseman toimintaperiaatteen muuttuminen. Vanhassa verkossa yhteinen verkkoasema oli kaikkien käytössä. Uudessa verkkoratkaisussa päädyttiin yhteiseen verkkoasemaan jossa oli kullekin organisaatiolle oma kansio, joka oli nimetty organisaation mukaisesti. Tähän kansioon organisaation jäsenillä oli täydet oikeudet ja muiden organisaatioiden jäsenillä vain luku -oikeudet. Suurin ongelma oli alkuun se, että hakemisto oli nimetty samoin, kuin organisaation oma verkkohakemisto. Näin osaa käyttäjistä huoletti alkuun väärälle asemalle tallentaminen vahingossa. Nopeasti käyttäjät kuitenkin omaksuivat uuden verkon toimintaperiaatteet ja sopeutuivat helposti Active Directory -verkkopalveluun.

## 6 YHTEENVETO

Opinnäytetyön tavoitteena oli luoda Mondo Mineralsille heidän käyttöönsä sopiva Active Directory -verkkojärjestelmä. Teoriaosuudessa käsiteltiin Active Directory ominaisuuksia, huomioitavia seikkoja toteutusta suunniteltaessa sekä Active Directoryn toimintaa järjestelmän ylläpitäjän näkökulmasta. Samalla esiteltiin toimeksiantajayritystä Mondo Minerals B.V. Branch Finlandia.

Active Directory -projekti alkoi tammikuussa 2008. CitiusNet Oy asensi virtuaalipalvelimet sekä niihin Active Directoryn ja sen tarvitsemat palvelut. Tämän jälkeen Active Directory -projekti eteni suunnittelun, testauksen ja muutaman erehdyksen jälkeen käyttöönottoon. Suunnittelu toteutettiin huolellisesti, joten lopputuloksena oli käyttötarkoitukseen sopiva AD-verkko.

Mondo Mineralsilla ennen käytössä ollut Novell Netware oli jo vanha, joten uuteen verkkoratkaisuun siirtyminen oli hyvä ratkaisu. Entinen verkko oli räjähtämässä käsiin ja Active Directory -verkkoon siirtyminen mahdollisti toimintatapojen muuttamisen sekä verkkorakenteen siivoamisen.

Uuden verkon myötä muutettiin toimintatapoja radikaalisti. Ennen verkossa oli paljon ylimääräisiä tiedostoja ja käyttäjiäkin, joita ei käytetty. Verkkouudistuksen myötä nämä ylimääräiset tiedot saatiin poistettua verkosta.

Entiseen Novell -aikaan verrattuna toimintatavat esimerkiksi käyttöoikeuksien luomisen suhteen muuttuivat miltei täysin toisenlaisiksi. Uudessa verkossa oikeuksia lisättäisiin ryhmien kautta luomalla Users and Computers -hallintakonsolin kautta. Ryhmä liitetään haluttuun hakemistoon ja saa näin vain tarvittavat oikeudet.

Vanhassa Novellissa myös nimeämiskäytäntö käyttäjätunnuksien luonnissa oli erilainen, kuin uudessa Active Directory -verkossa. Samoin myös organisaatioyksiköiden (OU) sekä ryhmien nimeämiskäytäntöjä muutettiin siten, että nimi viittaa jo suoraan hakemistoon, johon ryhmällä on oikeudet. Organisaatorakennetta muutettiin heijastamaan yrityksen omia organisaatioyksiköitä.



Entisessä Netwaressa käyttäjien ja ryhmien oikeuksien dokumentointi oli jäänyt jossain välissä tekemättä, joten vanhasta verkosta ei ollut enää yhtä ainoaa, yksiselitteistä dokumenttia, josta olisi nähnyt kunkin käyttäjän tai ryhmien oikeudet selkeästi. Uudessa verkossa toimintatapaa muutettiin siten, että kaikki tehdyt tunnukset, levyjaot ja ryhmät dokumentoidaan Excel -taulukkoon josta voidaan käydä helposti tarkistamassa oikeudet. Oikeudet -taulukko helpotti suuresti ylläpitäjän työtä.

Active Directoryn myötä verkkopalvelut saatiin toimimaan kankean alun jälkeen erittäin hyvin. Haastatellessani hoitovapaalta palannutta mikrotukihenkilöä, hän oli sitä mieltä, että uusi verkko toimii käytössä hyvin. Kuitenkin hänen mieleensä tuli yksi asia, mikä oli Netwaren aikaan ollut paremmin; ennen verkkoon kirjautuminen virhetilanteissa oli helppoa suoraan työpöydän N -ikonista esimerkiksi koneen pudotessa verkosta. Active Directoryssä kirjautuminen tehdään koneelle uudelleen kirjautumalla, mikä vie entiseen verrattuna enemmän aikaa. Kuitenkin verkosta ”putoamisia” tapahtuu uuden verkkoratkaisun myötä yhä harvemmin.

Tulevaisuudessa Active Directoryllä on tarjota Mondolle monia mahdollisuuksia. Active Directory mahdollistaa mm. Hollannin toimialueen yhdistämisen Suomessa toimivan toimialueen kanssa. Myös ryhmäkäytäntöihin paremmin tutustuminen saattaisi helpottaa järjestelmän ylläpitäjän työtä, kun käyttäjiltä rajattaisiin oikeuksia tiukemmin. Active Directoryn mahdollistama profiilin siirto sekä sovellusten paketointi voisi olla mahdollista tulevaisuudessa.

## LÄHTEET

Anttonen Leena & Kilpeläinen Simo, 2007.

Active Directoryn käyttöönoton selvitys Kajaanin Kaupungin ympäristötekniselle toimialalle. Kajaanin ammattikorkeakoulu: Opinnäyte.

Expert Exchange, 2008. Domain group policy shows local policy:

[http://www.expertsexchange.com/Microsoft/Server\\_Applications/Q\\_24013179.html](http://www.expertsexchange.com/Microsoft/Server_Applications/Q_24013179.html) (Luettu 18.5.2009).

Kivimäki Jyrki, 2003. Inside Active Directory- verkonhallinta. Helsinki: Edita Prima Oy.

Kivimäki Jyrki, 2005. Windows Server 2003, Active Directory.

Jyväskylä: Gummeruksen Kirjapaino Oy.

Lintunen Kari, 2006. Työkaluja vanhentuneiden käyttäjä- ja tietokonetilien löytämiseen ja poistamiseen Active Directoryssä. Tampereen ammattikorkeakoulu: Tutkinto-työraportti.

Microsoft, 2008. Technet:

[http://technet.microsoft.com/en-us/library/aa997340\(EXCHG.65\).aspx](http://technet.microsoft.com/en-us/library/aa997340(EXCHG.65).aspx) (Luettu 18.5.2008).

Mondo Minerals Group, 2008. Konsernitiedote.

Oulun yliopisto, 2000. Tietokonejärjestelmien ylläpidon politiikka:

<http://www.oulu.fi/tietohallinto/tietoturva/sisalto/yllapito/politiikka.html#hyvatapa> (Luettu 18.5.2008).

Partanen Timo, 2007. Active Directory -kurssimateriaali.

Piipponen Ritva, 2008. We Talk Talc -yritysesittelymateriaali.

SSW, 2009. Knowledge Base:

<http://www.ssw.com.au/SSW/kb/KB.aspx?KBID=Q1877839> (Luettu 18.5.2009).

Stanek William R, 2003. Microsoft Windows 2003 asiantuntijan käsikirja.

Helsinki: Edita Prima Oy.

Techrepublic, 2008. Solution Database: Active Directory Domains And Trusts Console:

[http://articles.techrepublic.com.com/5100-22\\_11-5160515.html](http://articles.techrepublic.com.com/5100-22_11-5160515.html) (Luettu 18.5.2009).

Tietokone.fi, 2007. Artikkelit: Novell Netware 5.2:

<http://www.tietokone.fi/lukusali/artikkelit/98tk12/NETWARE.HTM> (Luettu 18.5.2009).

Tools4ever, 2009.

<http://www.tools4ever.com/products/monitormagic/tips/03.asp>  
(Luettu 18.5.2009).

Topsofts, 2008. Downloads:

[http://www.topsofts.com/product/95599/Novell\\_NetWare\\_Revisor.html](http://www.topsofts.com/product/95599/Novell_NetWare_Revisor.html)  
(Luettu 18.5.2009).

Turunen Matti, 2006. It-järjestelmän kehittäminen seurakuntaympäristössä:

Case, Ylöjärvenseurakunta. Tampereen ammattikorkeakoulu: tutkintotyöraportti.

Usertify, 2008: Article: How to create a subnet.

<http://www.ucertify.com/article/how-to-create-a-subnet.html> (Luettu 18.5.2009).